Journal of Engineering Sciences
Vol 13, Issue 06, June/2022
ISSN NO:0377-9254

A METHODOLOGY FOR SECURE SHARING OF PERSONAL HEALTH RECORDS IN THE CLOUD

K.E.V.S.Amulya *#1,* R.Raghuram *#2,* B.Krishna Reddy #3, M.Akhileswar #4,
K.Venkateswarulu #5, T.Narendra#6
#1 Assistant Professor,#2,3,4,5,6 B.Tech.,Scholors
Dept of Computer Science & Engineering, QIS Institute of Technology, Ongole,Prakasam(Dt)

Abstract-Cloud computing has become an essential aspect of the healthcare industry. Accessing medical records from a hybrid cloud environment presents significant security and privacy concerns. This study proposes a new, safe, hybrid system for electronic health records. Two effective encryption methods are combined in this framework to ensure fine-grained access control and data privacy. After using a vertical partitioning method to divide the health records, multi-authority and key-based encryption schemes are used to secure each section. While in the Public Domains (PUDs), multi-authority encryption schemes predominate, Personal Domains (PD) encryption schemes use keys (PSDs).
Together, they provide secure data access and authentication of users.. The Windows Azure Cloud Computing platform makes implementation easier.

Keywords— Privacy, security, Electronic health records, Hybrid cloud, Data access, Authentication.

I. INTRODUCTION

One of the most important advantages of cloud computing is its ability to store and distribute massive volumes of data internationally [1]. With the use of cloud computing, electronic health records (EHRs) may be simply and efficiently maintained, shared, and provide access to the personal health information of patients in a secure environment. Since it's so expensive to construct and maintain EHR systems, many healthcare companies are opting for cloud-based services, such as those offered by Google Health. Hybrid cloud deployments have boosted the interest of healthcare organisations in hosting their electronic health records (EHR) on hybrid infrastructures.
This development has exacerbated the issue of EHR access security and privacy. An efficient authentication system and fine-grained access control are critical to overcoming the obstacles posed by cloud computing and ensuring the integrity of medical data.
Encryption is the best way to do this and keep sensitive information safe.
The goal of this project is to provide a hybrid solution for securely and privately exchanging EHRs in a hybrid cloud environment. We use two ABE approaches to encrypt each patient's EHR file in order to enable fine grained access control for EHRs. For the rest of this document, the following is the structure:
A review of pertinent material concludes Section 2. Within Section 3, you'll find an evaluation of the best present option, as well as a discussion of the recommended alternative. Sections 4 and 5 include implementation specifics and a logical architecture for the proposed system. Section 6 examines the outcomes of the implementation. Section 7 focuses on the conclusion and future research.

II. RELATEDWORKS

A. The effect of cloud security and privacy on EHR systems.
Cloud computing has emerged as a new service paradigm in the recent decade, resulting in the construction of multiple cloud-based data centres as cost-effective platforms for hosting large-scale service applications. Medical data security and privacy have proven to be major challenges for service providers, despite the many advantages and services offered. Researchers have come up with a slew of solutions to this problem. The combination of statistical and cryptographic approaches presented by [2] has resulted in a realistic hybrid solution for safe cloud data access. Flexible and secure data access, as well as the preservation of privacy, are the primary goals of this architecture.
A safe Electronic Health Record (EHR) system has been a priority for others, who have concentrated on achieving cloud security standards via the protection of patient medical information and confidentiality as in [1]. Health Insurance Portability and Accountability Act [3]-compliant electronic health record system was developed by these researchers [1]. Health providers may now access their electronic health records securely

utilising a user-friendly framework provided by [4]. Strong authentication and efficient encryption methods are used to guarantee fine grained access control in this system.

B. Cloud EHR Architecture Survey for Mobile Devices

Several academics have also focused on designing the architecture for a mobile health cloud and offered a comprehensive evaluation of the issues that arise while using mobile devices.

Hybrid cloud-based encryption, mobile apps, and role-based access control are all combined in [5] to create a mobile health app. The confidentiality and anonymity provided by this method aids in the improvement and speed of medical services. An Open SOA web framework for mobile health applications should be developed [6]. Patients may access their vital signs through this system, which offers them with advice depending on their readings. As an example, [7] have provided a comprehensive analysis of the security requirements for transferring an electronic health system to the cloud, including the process, significant problems, and solutions to these issues. For example, they have outlined some of its most common problems, including reliance on other systems and systems that aren't as secure as they should be.

The authors of this procedure conducted a survey on secure data deletion strategies and classified them [8]. According to [9], the transfer of Personal health information systems to a cloud environment was studied in a different way. There have been several secure cloud-based electronic health systems examined, but the authors do not have a system that they believe is both highly secure and private, as well as inexpensive.

C. Maintain security using Efficient Encryption Algorithm.

Encryption algorithms and authentication techniques have a substantial impact on the privacy and security of health record access. Encryption algorithms and other authentication standards have been integrated into a variety of solutions by researchers in this area.

An in-depth investigation of several EHR encryption strategies has been conducted by [10]. It's possible to strengthen the security and access control of current technologies, such as [11]. Hybrid encryption methods, such as Advanced Encryption Standard (AES) and Multi Authority Attribute Based Encryption (MA-ABE), are proposed as a hybrid solution to this problem. As an example, [12] present a system that encrypts health records using Attribute Based Encryption methods in order to ensure their safety and integrity.

[13] There are several academics that are interested in securing cloud-based shared data from public verifiers. For auditing cloud data without downloading whole datasets, they've suggested the Oruta privacy protection approach, which is built on top of a ring signature and a computational and authentication procedure. Attribute-based encryption (ABE) and a binary search tree approach have been combined to provide a health record access system that is both efficient and safe. Authors may assure the safety and privacy of stored EHRs in hybrid clouds by using the effectiveness of Cipher Policy Attribute-based encryption. Harmony, a heterogeneity-aware dynamic capacity solution for cloud data centres, has been developed by [15] to reduce scheduling delays and maximise energy savings. In their paper, however, the authors suggest that additional research and implementation are needed in order to explore workload heterogeneity and physical machines in depth.

III. PROPOSED SYSTEM ARCHITECTURE

CURRENT SOLUTION OF ELECTRONIC HEALTH RECORD (EHR) IN HYBRID CLOUD WITH LIMITATION

In the current solution for EHRs in the Hybrid Cloud, the statistical and cryptographic technology for sharing medical data in the hybrid cloud are combined.Vertical data partition, data merging, and integrity assurance are all described in great detail in the current system. Privacy-preserving data publishing is one of those components that may be considered one of the most important aspects of the Vertical data partitioning method.Quasi-identifiers, plain text medical information, and explicitly identified data are partitioned in the original EMR file during vertical partitioning. An Advanced Encryption Method (AES) and plaintext for medical information is used to protect Quai-identifiers and explicit identifiers published in a hybrid cloud. This component's restriction is that it encrypts data using the Advanced Encryption Standard (AES). It is critical to have a fine-grained access control system and an effective authentication strategy in place in order to ensure the privacy of medical data and allow safe access through hybrid cloud. In terms of protecting sensitive information, Advanced Encryption Standards (AES) is the best option since it has an established track record. However, privacy protection and processing time are its main drawbacks [16]. In addition, while AES requires less computing time for modest quantities of data processing, computation time quickly rises as the data size expands [16]. Furthermore, the existing solution's implementation results demonstrate that it is inefficient for the sharing and access of medical data by concurrent users. The present approach also uses a standard

authentication mechanism to verify the recipient's identity. Figure 1 depicts the existing solution, its limitations, and suggested mitigations.

PROPOSED SECURITY AND PRIVACY PRESERVED ELECTRONIC HEALTH RECORD ACCESS USING HYBRID CLOUD.

Medical records can be accessed using a hybrid cloud model that provides security and privacy, according to the proposed model. With the current system's shortcomings in mind, an HSS-EHRS, or Hybrid Secure and Scalable Electronic Health Record Sharing, is being considered. The primary goal of our proposed framework is to provide secure, scalable, and privacy-preserving access to EHR data in a Hybrid Cloud. Based on the data access requirements of recipients, we divide the system into two distinct security domains: Public Domains (PUD) and Personal Domains (PSD). EHR data can be accessed by PUD recipients based on their professional role, such as doctors, nurses, insurance executives, etc. In the case of PSD, the data owners are family members or friends of the users. With the ABE Scheme, we use encryption in both domains. The Multi Authority ABE scheme is employed in the public domain for multiple "Attribute Authorities" (AAs). The Attribute Authorities, rather than the EHR owners, can provide secret keys to Public Domain users. An encryption mechanism called Key Policy Attribute Based Encryption (KP-ABE) is utilised for Personal Domains (PSDs). Using the proposed HSS-EHRS system, we enhance the present system's security and fine-grained access control features. Combining two effective encryption techniques enables fine grained access control and data privacy protection to overcome the current best solution's limitations. After vertical partitioning, the Quasi Identifiers and Explicit Identifiers are encrypted using multi-authority and key-based encryption techniques. Figure 2 depicts the proposed system's block diagram.The data owners in the proposed system use a vertical data partitioning mechanism to divide the EHR file into three tables: pseudo IDs, Explicit Identifiers, and a Medical Information table. Key Policy Attribute Based Encryption is used to encrypt the Quasi Identifier and Explicit Identifier tables, whereas Multi Authority Attribute Based Encryption is used to encrypt the access policy. Medical information and encrypted tables are then released in a hybrid cloud environment. The existing system's difficulty with user revocation is eliminated by the key policy-based encryption technique.It is also beneficial to adopt the MA-ABE scheme in order to boost the scalability and give fine grained access control to EHRs. It is possible to create the policy based on the access policy system's suggested parameters. Medical information may be accessed by data receivers in both PUDs and PSDs, depending on the dataset level. EHR owners may provide direct access to unencrypted medical records with the permission of the EHR owners. Data merging components allow receivers to combine medical information with either pseudo identifiers or explicit identities. After dividing the EMR file, AES encryption is used to encrypt Quasi Identifiers and Explicit Identifiers, and RSA encryption is used to encrypt the key. Users from both public and private domains (PUD and PUD) may use the proposed technique to encrypt their explicit identifiers and Quasi-identifiers under a role-based access control (PSDs). To protect their data, they use an MA-ABE encryption technique with PUD characteristics and a KP-ABE encryption method with a PSD attribute established in step 4. Data owners may provide limited access to their EHR files in the Personal Domain to whomever they consider close friends or family members. PSD users have varying levels of access privileges depending on their interpersonal connections. If you've ever had to escrow a security key for your data, you'll appreciate the advantages of a multi-domain and multi-authority structure, which benefits data owners while reducing the burden on public users.Instead than employing a standard approach to verify users, the suggested system makes use of security domains, making recipient verification more simpler than in the present solution.

IMPLEMENTATION OF HSS-EHRS SYSTEM.

With the help of Windows Azure Cloud, the HSS-EHRS system is now operational. We used Windows Azure Cloud to deploy our proposed system and made use of a Cloud web service Azure SQL database and Virtual Machines in Windows Azure Cloud. Our HSS-EHRS is being implemented in two stages.Encryption schemes like KP-ABE and MA-ABE are used in the first case for the EHR file and fine-grained access control in this case. The projected HSS-EHRS system's encryption time was cut in half thanks to this new encryption technology. The average response time for concurrent HTTP requests in the Windows Azure cloud was also examined. Specific design elements include EMR Attribute Classification and Key Distribution, which are critical.

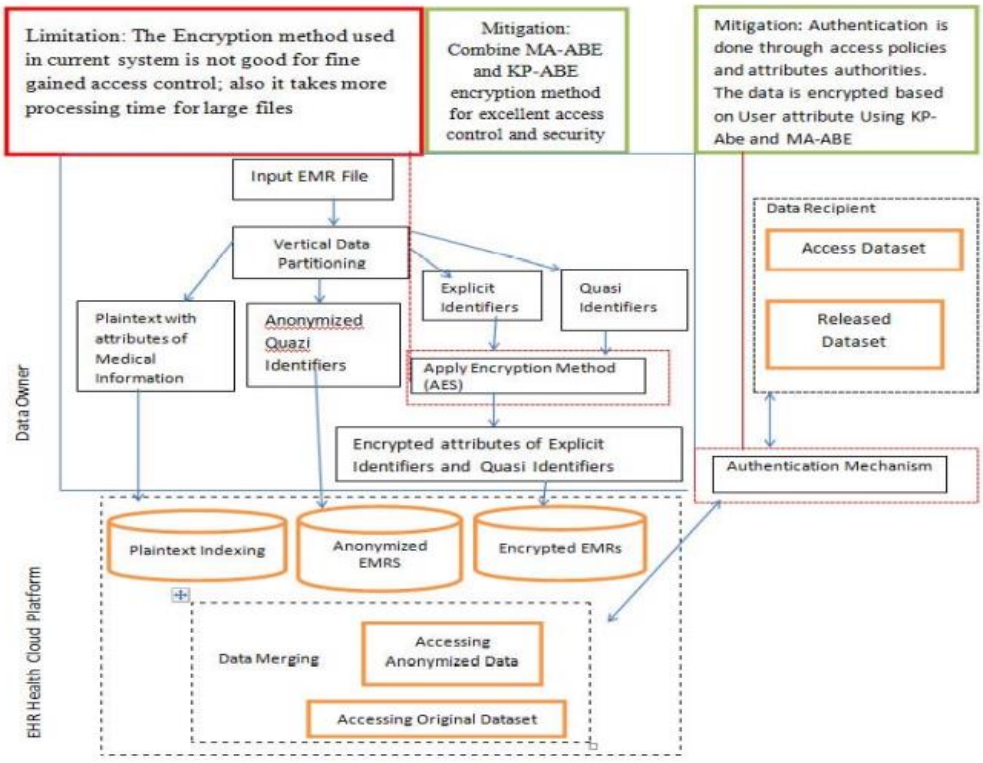

Fig. 1. Current system for Electronic Health Record in the Hybrid cloud

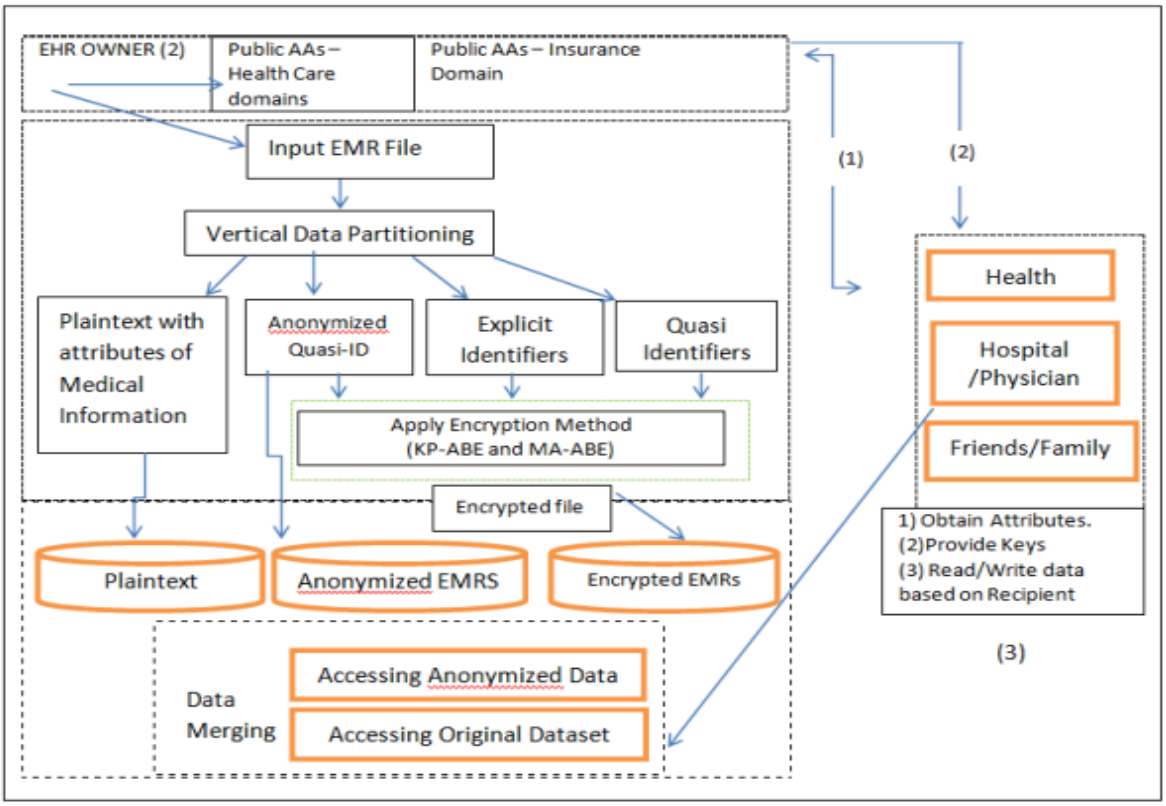

Fig. 2. Proposed System for Secure and Privacy Medical Data Access from Hybrid Cloud

Algorithm : **Electronic Health Record (EHR) Encryption Algorithm.**

INPUT : Electronic Health Record File (D); (D) = { $D_1, D_2 \ldots D_n$}.
Personal Domain Attribute Set (PSD);
PSD = {$A_{psd1}, A_{psd2}, \ldots, A_{psdn}$}, where A is attribute value of personal recipient.
Public Domain Attribute set (PUD); PUD = {A_{pud1}, $A_{pud2}, \ldots, A_{pudn}$}.

OUTPUT : Encrypted File (De); De = { $D_{e1}, D_{e2}, \ldots D_{en}$}
with attributes of EID and QID.

Plaintext (D_p); D_p = {D_{p1}, D_{p2}, ...D_{pn}) with attributes of medical information.

Anonymized table (D_a); D_a = { $D_{a1}, D_{a2}, \ldots D_{an}$} with attributes of QID.

Initials: The original Electronic Health Record (D), Quasi Identifiers (QID), Medical Information (MI), Explicit Identifiers (EID).
Assign NULL to both Da and De;

BEGIN:

Step 1: Input D,PUD and PSD;
Step 2: Encrypt QID and EID by extracting them from D;
For each i=1 and less than or equal to end of the record, n,
Repeat step 3 to 8 until end of the file reached.
Step 3: For each Aj element of EID U QID
Step 4: Dei(Aj)= E(KP-ABE)[Di(Aj)] Using PSD attribute set.
Dei(Ak)= E(MA-ABE)[Dk(Aj)] Using PUD attribute set.
Step 5: Extract MI from D and store in Dp, as plaintext.
For each Aj element of MI
Dpi(Aj)= Di(Aj).
Step 6: Increment the value of i.
Step 7: Process the K-anonymization Partition for extracting QID from D.
Step 8: For I =1 and less than or equal to end of the record, repeat the until end of the file reached.
Step 9: For each Aj belong to QID
Dai(Aj) = Range (Ek), where di belongs to Ek.
Step 10: Store Output Da,Dp and De separately in Hybrid cloud
Step 11: END.

IV. RESULTS AND DISCUSSION

A.Encryption time affects efficiency.

Experiment results on EHR encryption are shown in table 1. Cipher text for both current and proposed systems only encodes the attribute values of Explicit (EID) and Quasi Identifiers (QID). We ran the test on a variety of EHR sizes. Using an AES method with a key length of 128 for the current system, the data is encrypted. The attribute values are encrypted with an Attribute based encryption method in the proposed system. Using Key policy Attribute based encryption in the private domain and Multi–Authority attribute based encryption in the public domain, respectively, is the preferred way. Table 1 below shows the encryption time for the present and planned systems. The suggested system encryption time is based on the following parameters: Exp1=6.4ms, ExpT=0.6ms, and pairing time=2.5 ms. The encryption time and security of the existing system are reliant on the length of the key and the number of pairings. Implementing both present and suggested encryption methods in java programming language was necessary to carry out this experiment.

B.Users in the Windows Azure cloud should expect an average response time of under one second for HTTP requests.

Measurements of average response time for HTTP requests in private and public domains are shown on the following table 2. In this experiment, we used Cloud web services, Azure SQL databases, and Virtual machines to deploy our proposed system in the Windows Azure Cloud. This experiment began with a large SQL database and a Virtualized Web service that could handle any service request. Workload generation tools are used by concurrent users to access the system. Twenty different user groups from the public and private domains are simulated using Apache JMeter, a workload generation tool. Windows Azure Cloud hosts our proposed system, and this helps us evaluate its scalability. Our proposed system with Windows Azure Cloud configuration provides the best Quality service in terms of response time for

HTTP requests for web service and query processing, as can be seen in tableau 4. Each patient (data owner) utilises the KP-ABE scheme for initialization, key generation, and key revocation in the proposed algorithm. KP-ABE and MA-ABE are used to encrypt Electronic Health Records, ensuring that they cannot be read by anyone other than the cloud service provider. It also aids in the maintenance of the resistance to collusion. Our proposed system's decryption is blazingly fast, thanks to the use of only (Apud)+1 pairing operations. As the number of attributes increases, so does the amount of time it takes to encrypt and decrypt, and the cost of key generation. It takes less than 500 milliseconds for 10 attributes.

Because it ensures a unified security framework for EHR sharing in multi-domain with numerous users, the proposed system stands in sharp contrast to the existing one. EHR can be accessed in both the public and private domains using this framework's strong access control mechanism. For each EHR system, the proposed solution allows users to choose their own access policy. With the help of our new framework, data owners may provide access to their EHRs to both personal and public users, with varied responsibilities, using the ABE scheme for EHR encryption.

TABLE I. ENCRYPTION TIME FOR CURRENT AND PROPOSED SYSTEM

Input: EHR		No.of Attributes	Encryption Time(ms)	
Type	*Size(Mb)*		*Proposed system*	*Current solution [2]*
.doc	1	30	1593	4126.8
.txt	5	35	4403.4	18378.4
.xlsx	10	40	5237.9	19671.9
.Xlsx	20	45	6994.7	21899.3
.txt	50	50	8750.4	24470.7
.txt	70	55	10506.5	27442.4
.txt	100	60	12261.3	29906.6
.txt	150	65	15752.9	35441.3
.doc	200	70	17338.7	41198.9
.doc	250	75	19093.5	46150.2
.doc	300	80	21028.1	50423.8
.doc	350	85	22717.6	55785.4
.txt	400	90	24474.5	59653.2
.txt	450	95	26230.2	64867.1
.txt	500	100	28167.3	68247.2
.txt	550	105	29852.5	73112.8
.txt	600	110	31608.4	77599.5
.doc	650	115	32962.8	85743.2
.doc	700	120	35297.5	91870.5
.doc	750	125	37904.7	95976.9

TABLE II. ENCRYPTION TIME FOR CURRENT AND PROPOSED SYSTEM

Number of Users	Average response time of HTTP request (MS)	
	Proposed System	*Current solution [2]*
1	120	133
6	135	139
12	153	157
18	172	177
22	190	198
25	195	201
30	202	205
32	216	223
38	224	230
40	235	241
46	242	252
52	255	260
58	263	273
64	274	284
72	286	295
80	297	309
85	312	319
94	321	332
98	336	349
110	353	366

V. FUTURE SCOPE AND CONCLUSION

Cloud-based EHR management is a new area of IT research. Concerns about the security and privacy of data while it is stored and accessed remain. More and more researchers have come up with and put into action a wide range of security and privacy techniques in recent years. Despite this, conventional approaches are typically insufficient to protect data in a hybrid cloud.

Electronic health records (EHRs) may be securely shared in a hybrid cloud environment by using two cryptographic methods: a public key encryption (PKI) and an elliptic curve cryptography (ECC). Using an ABE encryption approach, the EHR files are encrypted using a two-domain security division. On the basis of encryption times and concurrent recipient data access and sharing, the system's efficiency was shown to be effective. The improved MA-ABE encryption technique can handle on-demand recipient data access while still delivering high levels of security. It is.

REFERENCES

[1] Y. Chen, J. Lu and J. Jan, "A Secure EHR System Based on Hybrid Clouds," Journal of Medical System, vol. 36, no. 5, p. 3375–3384, 2014. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[2] J. J. Yang, J. Li and Y. Niu, "A Hybrid solution for privacy preserving medical data sharing in cloud computing.," Future Generation computer systems, vol. 43, no. 44, pp. 74-86, 2015.
[3] HIPPA, "104th United States Congress, Health Insurance Portability and Accountability Act of 1996 (HIPPA) 1996.," 1996. [Online]. Available: http://aspe.hhs.gov/admnsimp/pl104191.htm.
[4] B. Coats and S. Acharya. S, "Bridging Electronic Health Record Access to the Cloud.," IEEE 47th Hawaii International Conference on System Science., pp. 2948-2957., 2014.
[5] K. Nagaty, "Mobile Health Care on a Secured Hybrid Cloud.," Cyber Journals, vol. 4, no. 2, 2014.
[6] J. Meyer, "Open SOA Health Web Platform for Mobile Medical Apps: Connecting Securely Mobile Devices with Distributed Electronic Health Records and Medical Systems," IEEE, pp. 1-6, 2014.
[7] A. Michalas, N. Paladi and C. Gehrmann, "Security Aspects of eHealth Systems Migration to the Cloud," IEEE 16th International Conference on e-Health Networking, pp. 212-218, 2014.
[8] J. Reardon, D. Basin and S. Capkun, ""Sok: Secure data deletion," in SecurityandPrivacy(SP)," IEEESymposiumon, pp. 301-315, 2013.
[9] H. Aljafera, Z. Malika and M. Alodibb, "A brief overview and an experimental evaluation of data confidentiality measures on the cloud," Journal of Innovation in Digital Ecosystems, vol. 1, no. 1-2, pp. 1-11, December 2014.
[10] S. Lu, R. Ranjan and P. Strazdins, "Reporting an experience on design and implementation of e-Health systems on Azure cloud.," CSIRO Computational Informatics., vol. 27, no. 10, pp. 2602-2615., 2015.
[11] M. N. Shrestha, A. Alsadoon, C. P. Prasad and Houran, "Enhanced eHealth Framework for Security and Privacy in Healthcare.," IEEE, pp. 75-79., 2016.
[12] S. Suresh, "Highly Secured Cloud Based Personal Health Record Model.," International Conference on Green Engineering and Technologies (IC-GET), pp. 1-4, 2015.
[13] B. Wang, . B. Li and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," IEEE 5th International Conference, pp. 295-302., 2012.
[14] Z. Liu, J. Weng, J. Li, J. Yang, C. Fu and C. Jia, "Cloud-based electronic health record system supporting fuzzy keyword search," Soft Computing, vol. 20, no. 8, p. 3243–3255, 2016.
[15] Q. Zhang, M. F. Zhani, R. Boutaba and J. L. Heller, "Harmony: Dynamic Heterogeneity-Aware Resource Provisioning in the Cloud," IEEE 33rd International Conference, pp. 510-519., 2013